



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,650	12/20/2001	Anton C. Rothwell	NAIIP056/01.187.01	2721
28875	7590	07/29/2009		
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			EXAMINER CHEA, PHILIP J	
			ART UNIT 2453	PAPER NUMBER
			NOTIFICATION DATE 07/29/2009	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

anita@zilkakotab.com
erica@zilkakotab.com
dottie@zilkakotab.com

Office Action Summary	Application No. 10/028,650	Applicant(s) ROTHWELL ET AL.	
	Examiner PHILIP J. CHEA	Art Unit 2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-7,12-14,16-20,25-31,33-41,43 and 44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-7,12-14,16-20,25-31,33-41,43 and 44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>3/18/09; 5/22/09</u> | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2453

DETAILED ACTION

This Office Action is in response to an Amendment filed October 28, 2008. Claims 1,3-7,12-14,16-20,25-31,33-41,43-44 are currently pending. Any rejection not set forth below has been overcome by the current Amendment.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1,3,4,7,12-14,16-17,20,25-31,34,38-40,43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan et al. (US 6,075,863), and further in view of Chi (6,006,329), and further in view of Lerche et al. (US 5,511,163), herein referred to as Lerche, and further in view of VirusScan for Windows 95 User's Guide, herein referred to as VirusScan further in view of Foss et al. (US 6,298,444), herein referred to as Foss, from IDS filed 3/18/09.

As per claim 1, Krishnan discloses a network adapter system, comprising:

a processor positioned on a network adapter coupled between an end-point computer and a network (see column 2, lines 33-39, where network adapter is considered the software-controlled modem), the network adapter capable of being installed on the end-point computer (see column 2, lines 44-50);

wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses (see column 5, lines 16-28, where processor executes applets to scan incoming data such as hazardous programs and viruses and content is considered "junk e-mail");

Art Unit: 2453

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses).

Although the system disclosed by Krishnan shows substantial features of the claimed invention (discussed above), it fails to disclose that the virus scanning utilizes virus signature files and that the virus signature files are stored on non-volatile solid state memory on the network adapter.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan, as evidenced by Chi.

In an analogous art, Chi discloses scanning data streams for viruses (see Abstract) using virus signature files to detect known viruses (see column 3, lines 47-65).

Given the teaching of Chi, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan by employing virus signatures, such as disclosed by Chi, in order to detect the viruses without having to store the entire virus code.

In considering the virus signature files being stored on non-volatile solid state memory on the network adapter, Krishnan shows storing virus detection applets and program code implementing a virtual machine for execution of programs in ROM and battery backed RAM for long term storage (see column 2, line 65 – column 3, line 12). Therefore it would be obvious to also store the virus signature files with the applets and program code in order for the applets executing the virus scan to use the signatures to detect viruses.

Although the system disclosed by Krishnan in view of Chi shows substantial features of the claimed invention (discussed above), it fails to disclose that a predetermined amount of the received

Art Unit: 2453

packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi as evidenced by Lerche.

In an analogous art, Lerche discloses a system with a computer and a network adapter that is able to receive all information on the network and the adapter can perform an assembling and scanning of all files on the network and carry out a recognition of virus signatures (see Abstract). Lerche also discloses that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter (see column 1, lines 38-49, *showing that a predetermined amount of packets (i.e. amount of packets making up the one file that is scanned) are assembled into one file and then determined if they are of interest by scanning them for detection of virae and the packets are received at a network adapter in order to intercept the packets and scan them*).

Given the teaching of Lerche, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi by employing assembling of the received packets, such as disclosed by Lerche, in order to catch all potential viruses on a network of computers.

Although the system disclosed by Krishnan in view of Chi in view of Lerche shows substantial features of the claimed invention (discussed above), it fails to disclose that if the received packets that are interest fail the scanning, an alert is displayed which provides remedy options.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche, as evidenced by VirusScan.

In an analogous art, VirusScan discloses a prompt for action when a virus is found (i.e. file has failed the scanning) where an alert is displayed which provides remedy options (see page 47 "Removing a Virus"). VirusScan further discloses that if a virus is found the remedy options are to "stop", "clean" and "delete" (see page 47).

Art Unit: 2453

Given the teaching of VirusScan, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche by employing remedy options, such as disclosed by VirusScan, in order to aid in a fix for the infected computer.

Although the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan shows substantial features of the claimed invention (discussed above), it fails to disclose wherein the received packets are of interest based on an associated protocol.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan, as evidenced by Foss.

In an analogous art, Foss discloses a system disclosed for providing enhanced computer network security by scanning data sent to the network before the data is received and transmitted (see Abstract). Foss further discloses determining whether received packets are of interest (see Fig. 4A [402], *showing if the packet is associated with a known protocol i.e. are they of interest*) and wherein the packets are of interest based on an associated protocol (see Fig. 4A [406] and [402], *if they are based on a known protocol they are passed through*).

Given the teaching of Foss, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche in view of VirusScan by determining if packets are of interest based on an associated protocol, such as disclosed by Foss, in order to determine if an email message is being sent through a known protocol that is acceptable for mail transmission and translation.

As per claims 3,16, Krishnan discloses that the processor is capable of being user-configured locally (see column 3, lines 24-26)

As per claims 4,17, Krishnan further discloses that the processor is capable of being user-configured remotely via a network connection with the network adapter (see column 3, lines 36-37).

Art Unit: 2453

As per claims 7,20, Krishnan further discloses that the settings of the network adapter are capable of being user-configured (see column 5, lines 33-35).

As per claims 12,25, Krishnan further discloses that the processor is capable of denying received packets that fail the scan (see column 5, lines 16-23).

As per claims 13,26, Krishnan further discloses that the scan is performed based on user settings (see column 3, lines 2-6).

As per claims 14,27, Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss disclose a method for scanning network traffic on a network adapter, comprising:

receiving packets at a network adapter including a processor positioned thereon, the network adapter being capable of being installed on an end-point computer (see Krishnan column 2, lines 33-39, where network adapter is considered the software-controlled modem);

virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses (see Krishnan column 5, lines 16-28, where processor executes applets to scan incoming data and content is considered "junk e-mail"); and

conditionally taking security measures if the packets fail the scan (see Krishnan column 5, lines 16-23);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a

Art Unit: 2453

virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses);

wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter (see Lerche column 1, lines 38-49);

wherein if the received packets that are of interest fail the scanning, an alert is displayed which provides remedy options (see VirusScan page 47);

wherein the received packets are of interest based on an associated protocol (see Foss, Fig. 4A [402][406]).

As per claim 28, Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss disclose a method for scanning network traffic on a network adapter, comprising:

receiving packets at a network adapter including a processor positioned thereon, the network adapter being capable of being installed on an end-point computer (see Krishnan column 2, lines 33-39, where network adapter is considered the software-controlled modem);

virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses (see Krishnan column 5, lines 16-28, where processor executes applets to scan incoming data and content is considered "junk e-mail"); and

conditionally taking security measures if the packets fail the scan (see Krishnan column 5, lines 16-23);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

Art Unit: 2453

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses);

wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter (see Lerche column 1, lines 38-49);

wherein scanning the received packets that are of interest is prioritized based on a file type associated with the received packets (see VirusScan page 26, where certain file types can be chosen for scanning over other file type i.e. the chosen file types have priority over the other file types);

wherein the received packets are of interest based on an associated protocol (see Foss, Fig. 4A [402][406]).

As per claim 29, Krishnan in view of Chi in view of Lerche in view of VirusScan disclose a network adapter system, comprising:

a processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module (see column 2, lines 56-65, where it is implied if not inherent that there is a packet assembly module in order to receive data from the outside see column 5, lines 16-18 for scanner module);

a user interface driver for identifying network traffic of interest transmitted between the computer and the network (see Krishnan column 5, lines 24-31);

Art Unit: 2453

wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the computer and the network (see Krishnan column 5, lines 16-31);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

wherein the network adapter receives the network traffic (see Krishnan column 5, lines 16-23);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses);

wherein a predetermined amount of the received network traffic is assembled for determining whether the received network traffic is of interest, the received network traffic including network traffic received at the network adapter (see Lerche column 1, lines 38-49);

wherein scanning the received network traffic of interest is prioritized based on a file type associated with the received network traffic (see VirusScan page 26, where certain file types can be chosen for scanning over other file types i.e. the chosen file types have priority over the other file types);

wherein the received packets are of interest based on an associated protocol (see Foss, Fig. 4A [402][406]).

Art Unit: 2453

As per claim 30, Krishnan further discloses that the content scanning enforces operational policies of an organization (see column 5, lines 24-30).

As per claims 31,40, Krishnan further discloses that the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation (see column 5, lines 24-30).

As per claim 34, Krishnan further discloses that the packets that are of interest include executable files (see column 5, lines 16-23).

As per claim 38, Krishnan further discloses that the network adapter includes a cable modem adapter (see column 6, lines 36-45).

As per claim 39, Krishnan further discloses that the network adapter includes a broadband adapter (i.e. cable modem).

As per claim 43, Foss further discloses that the received packets that are not of interest to the end-point computer bypass the scanning (see Foss, Fig. [402][406]).

3. Claims 5,18,33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss as applied to claims 1,14 above, and further in view of Bonomo et al. (US 6,658,562), herein referred to as Bonomo.

As per claims 5,18,33, although the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss shows substantial features of the claimed invention (discussed above), it fails to disclose that memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss, as evidenced by Bonomo.

In an analogous art, Bonomo discloses a system for setting different BIOS configurations stored in a memory device (see Abstract). Further showing setting a password to view information in a BIOS setup program or to change configuration (see column 4, lines 11-21 and 30-41).

Art Unit: 2453

Given the teaching of Bonomo, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss by employing a password protected BIOS, such as disclosed by Bonomo, in order to prevent unwanted users from changing settings without authorization.

4. Claims 6,19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss as applied to claim 1 above, and further in view of Templeton (US 6,401,210).

Although the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss shows substantial features of the claimed invention (discussed above), it fails to disclose that the manner in which the scanning performed is user-configured.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss, as evidenced by Templeton.

In an analogous art, Templeton discloses a system for managing files infected by computer viruses (see Abstract). Further disclosing that the manner in which the scanning performed is user configured (see column 4, lines 8-35, describing scan options that are user configured).

Given the teaching of Templeton, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss by employing user configured scan options, such as disclosed by Templeton, in order to perform specific actions when a virus is detected.

5. Claims 35-36, are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss.

As per claim 35,36, Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss does not expressly disclose that the network adapter includes a Peripheral Component Interconnect (PCI) card and/or an Industry Standard Architecture (ISA) card. However, Krishnan does disclose that the

Art Unit: 2453

adapter can be an add-in card for installation in an expansion slot of a computer comprising an expansion bus interface (see column 2, lines 47-50). At the time of the invention, a person having ordinary skill in the art would have recognized that PCI and ISA are commonly used and well known expansion bus interfaces. Therefore it would have been obvious to make network adapters for both PCI and ISA in order to provide an adapter compatible with most computers.

6. Claims 35-37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss as applied to claim 1 above, and further in view of Sridhar et al. (US 5,799,064), herein referred to as Sridhar.

As per claims 35,36 although the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss shows substantial features of the claimed invention (discussed above), it fails to disclose that the network adapter includes a Peripheral Component Interconnect (PCI) card and/or an Industry Standard Architecture (ISA) card.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss, as evidenced by Sridhar.

In an analogous art, Sridhar discloses an apparatus interfacing between a communication channel and a processor for data transmission and reception (see Abstract) further showing that the apparatus may be connected to a bus such as an ISA or PCI bus (see column 3, line 63 – column 4, line 2).

Given the teaching of Sridhar, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss by employing a network adapter including a PCI and/or ISA card, such as disclosed by Chi, in order to connect to the bus of the end-point computer.

As per claim 37, Sridhar further discloses that the network adapter includes an Integrated Services Digital Network (ISDN) adapter (see column 4, lines 11-19).

Art Unit: 2453

7. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss as applied to claim 1 above, and further in view of Horvitz et al. (US 6,161,130), herein referred to as Horvitz..

Although the system disclosed by Krishnan shows unwanted content includes junk e-mails and misinformation (see column 5, lines 24-25 for junk e-mail and column 5, lines 16-18, where Trojan horses are considered misinformation), it fails to disclose harassing content and pornographic content.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss, as evidenced by Horvitz.

In an analogous art, Horvitz discloses a system that detects electronic mail messages that the recipient is likely to consider junk (see Abstract). Further disclosing that the unwanted messages include harassing content and pornographic content (see column 9, lines 44-51, where harassing content is considered abusive or insulting messages).

Given the teaching of Horvitz, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss by employing a harassing content and pornographic content filter, such as disclosed by Horvitz, in order to keep the incoming data safe for users.

8. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss as applied to claim 29 above, and further in view of Maher, III et al. (US 6,910,134), herein referred to as Maher.

Although the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss shows substantial features of the claimed invention (discussed above), it fails to disclose that the packet assembly module utilizes header information associated with received packets for assembling data fields of the received packets.

Art Unit: 2453

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss, as evidenced by Maher.

In an analogous art, Maher discloses a system for detecting and inoculating email infected with viruses (see Abstract). Maher goes into further detail about a packet assembly module to reassemble data packet fragments and how the header information is utilized to assemble the packets (see column 4, lines 47-59).

Given the teaching of Maher, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Lerche in view of VirusScan in view of Foss by employing a header pre-processor to assemble data fields of the received packets, such as disclosed by Maher, in order to scan the payload for known virus signatures.

Response to Arguments

9. Applicant's arguments with respect to claims 1,3-7,9,12-14,16-20,22,25-31,33-41,43-44 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHILIP J. CHEA whose telephone number is (571)272-3951. The examiner can normally be reached on M-F 6:30-4:00 (1st Friday Off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2453

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Philip J Chea
Examiner
Art Unit 2453

/Philip J Chea/
Examiner, Art Unit 2453
7/21/09